# PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

## PCT

### NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

| | |
|---|---|
| **Date of mailing** (day/month/year)<br>10 November 2000 (10.11.00) | |
| **International application No.**<br>PCT/DE00/00189 | **Applicant's or agent's file reference**<br>990202PCT |
| **International filing date** (day/month/year)<br>20 January 2000 (20.01.00) | **Priority date** (day/month/year)<br>29 March 1999 (29.03.99) |
| **Applicant**<br>BRESSER, Bertram et al | |

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

12 October 2000 (12.10.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

**The International Bureau of WIPO**
**34, chemin des Colombettes**
**1211 Geneva 20, Switzerland**

Facsimile No.: (41-22) 740.14.35

Authorized officer

Christelle Croci

Telephone No.: (41-22) 338.83.38

Translation

# PATENT COOPERATION TREATY

# PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

9193819

| Applicant's or agent's file reference 990202PCT | FOR FURTHER ACTION | See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) |
|---|---|---|
| International application No. PCT/DE00/00189 | International filing date (*day/month/year*) 20 January 2000 (20.01.00) | Priority date (*day/month/year*) 29 March 1999 (29.03.99) |

International Patent Classification (IPC) or national classification and IPC
H04L 9/30

Applicant
FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.



3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

| Date of submission of the demand | Date of completion of this report |
|---|---|
| 12 October 2000 (12.10.00) | 31 May 2001 (31.05.2001) |
| Name and mailing address of the IPEA/EP<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE00/00189

**I. Basis of the report**

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-20, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. 2-11,13-16, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1,12, filed with the letter of 25 April 2001 (25.04.2001),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/1, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

| | | | |
|---|---|---|---|
| Novelty (N) | Claims | 1-16 | **YES** |
| | Claims | | **NO** |
| Inventive step (IS) | Claims | 1-16 | **YES** |
| | Claims | | **NO** |
| Industrial applicability (IA) | Claims | 1-16 | **YES** |
| | Claims | | **NO** |

2. Citations and explanations

1- According to its title, the international application PCT/DE00/00189 is directed to a device and method for secure electronic data processing. Claim 1 lays claim to the device and independent Claim 12 to the method.

2. According to the international search report, documents **D1** and **D2** represent the **closest prior art.**

**D1:** EP-A-0 869 652 (TUMBLEWEED SOFTWARE CORP.), 7 October 1998 (1998-10-07)

**D2:** US-A-5 751 813 (DORENBOS DAVID), 12 May 1998 (1998-05-12).

The preamble of Claim 1 is based on the disclosure of D2.

The disadvantage of the prior art is explained on page 2, paragraphs 2 and 3, and also on page 6, lines 15-31.

3. **The invention addresses the problem** (page 2, last paragraph) of providing a device and method for secure data transmission via a network server, in

which the data addressee need not yet be known at the time the data are provided.

4a) This problem is solved by the advantageous interaction of the technical features indicated in Claim 1. The device as per Claim 1 is depicted in the figure.

Claim 1 reads:

Device for the secure transmission or forwarding of encrypted data
from a first data station
via a second data station
to a third data station in a network,
said device comprising

- an input unit for receiving the encrypted data (10a) from the first data station and an external requestor key from the third or further data station;
- a unit (2) for re-encrypting the encrypted data by decrypting with an internal key and re-encrypting with the external key, the internal key being inaccessible from outside of the device; and
- an output unit for outputting the data (10b) encrypted with the external key,

**characterised in that**
the device is designed *in such a way* on or in the second data station that the unit (2) re-encrypts the data *only* when requested by the third data station, using the external requestor key, and the data do not leave the device during re-encryption, and therefore are not accessible in a non-encrypted form outside the device at the second data station.

4b) The problem addressed by the invention is solved by the advantageous interaction between the technical features indicated in independent Claim 12. Claim 12 reads:

method for the secure transmission of data
from a first data station
via a second data station
to a third data station
using the *device according to one of the preceding claims* at or in the second data station, said method comprising the following steps:

- encryption of the data **in the first data station** using a first key (10a);
- subdivision of the first key (10a) into a first part and a second part, so that neither part alone enables the encrypted data to be decrypted;
- encryption of the first part of the first key (10a) in the first data station using the public key of the second data station;

- transmission of the encrypted data (11), together with the encrypted first part of the first key (10a), to the second data station;
- storage of the encrypted data (11) and of the encrypted first part of the first key (10a) **in the second data station**;
- data request by the third data station, which is identified to the second data station only when it places the request;
- decryption of the encrypted first part of the first key in the second data station using a private key of the second data station that fits the public key; and

re-encryption of the previously decrypted first part of the first key with a public key of the third data station; and

- transmission of the encrypted data (11), together with the re-encrypted first part of the first key (10b), to the third data station;

- decryption of the encrypted first part of the first key (10b) **in the third data station** using a private key that fits the public key of the third data station;
- completion of the first key (10a) by completing in the third data station the first part of the first key with the second part of the first key, which was transmitted over a separate path from the first to the third data station;
- decryption of the encrypted data (11) using the completed first key (10a) in the third data station.

5. The subjects described in Claims 1 and 12 have advantageous effects, as explained on page 7 (last paragraph) of the description.

6. **No** international search report citation alone discloses the totality of the technical features of Claim 1 and independent Claim 12. The subject matter of Claims 1 and 12 therefore meets the requirements of PCT Article 33(1) and (2) for novelty. The international search report also **fails to suggest** the subject matter of Claims 1 and 12. The requirements of PCT Article 33(1) and (3) for inventive step in the claimed subject matter are therefore met.

The subject matter of Claims 1 and 12 is industrially applicable, *inter alia*, in the field of transmission of medical data. Consequently, the requirements of PCT Article 33(1) and (4) for industrial applicability are met.

7. Dependent Claims 2-11 and 13-16 define special configurations of the device as per Claim 1 and method as per Claim 12, respectively, which in principle and subject to the observations in Box VIII, also meet the requirements of PCT Article 33(2)-(4) for novelty, inventive step and industrial applicability.

**VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1(a)(ii), the description does not cite documents **D1** and **D2** and does not indicate the relevant **prior art** disclosed therein.

2. Contrary to PCT Rule 5.1(a)(iii), the **description** (page 3, paragraphs 2 ff.) is not in line with the claims.

3. Certain expressions, such as "receivers p'key", which are not in the language of the proceedings (German) and do not fall under the category of known technical expressions, are used in Figure 1/1. These expressions should be replaced by comprehensible terms in the selected language of the proceedings. The English terms may still be used, if placed between parentheses after the German terms.

The applicant has stated his intention to carry out the corresponding amendments and corrections when the application enters the regional or national phase.

**VIII Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

The original dependent Claims 2-11 and 13-16 have not been made consistent with the amended independent Claims 1 and 12. Consequently, some objections are raised under PCT Article 6 because the additional features of the dependent claims cause a lack of clarity (for example, Claim 13) or because the additional features of the dependent claims have become superfluous (for example, Claims 14 and 15), and hence the claims are no longer concise.

The applicant has stated his intention to carry out the corresponding amendments and corrections of the dependent claims when the application enters the regional or national phase.

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT [redacted] DEM GEBIET DES PATENTWE[redacted]S

# PCT

## INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

| Aktenzeichen des Anmelders oder Anwalts<br>990202PCT | **WEITERES VORGEHEN** | siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5 |
|---|---|---|
| Internationales Aktenzeichen<br>PCT/DE 00/ 00189 | Internationales Anmeldedatum *(Tag/Monat/Jahr)*<br>20/01/2000 | (Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*<br>29/03/1999 |
| Anmelder<br>FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG.et al | | |

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [ ] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

International Preliminary Examining Report of 31/05/01

1. This internal preliminary examining report is issued by the Office assigned therewith and is forwarded to the applicant in accordance with Article 36.

2. This report comprises all told 8 pages including the cover page.

   Moreover. The report is accompanied by ENCLOSURES; these are pages with specification, claims and/or drawings which have been altered and are the basis of this report, and/or pages with amendments made before this authority (see Rule 70.16 and Section 607 of the Guidelines for PCT)

   These enclosures comprise all told 3 pages.

| | | |
|---|---|---|
| I | X | Basis of the report |
| V | X | Reasoned opinion according to Rule 35(2)regarding novelty, inventive step and commercial applicability: documents and explanation in support thereof |
| VII | X | Specific shortcomings of the international application |
| VIII | X | Specific remarks concerning the international application |

**I. Basis of the Report**

1.This report was drawn up on the basis (replacement pages filed upon request by the Office according to Article 14 shall be considered within the scope of this report as "originally filed".)

**Specification, Pages:**
1-20 original version

**Claims, Nos.:**
2-11,13-16 original version

1,12 submitted on 25/04/2001 with letter of 24/04/2001

**Drawings, pages:**
1/1 original version

**V. Reasoned opinion to according Rule 66.2a)ii) regarding novelty, inventive step and commercial applicability: documents and explanation in support thereof**

1. Opinion

| | |
|---|---|
| Novelty (N) | Yes: Claims 1-16 |
| Inventive step (IS) | Yes: Claims 1-16 |
| Commercial applicability (CA) | Yes: Claims 1-16 |

2. Documents and Explanations
**see accompanying page**

**VII. Specific shortcomings of the international application**
It was determined that the international application shows the following shortcomings as to form and content:
**see accompanying page**

**VIII. Specific remarks concerning the international application**
For clarity of the claims, of the specification and the drawings or whether or not the claims are fully supported by the specification, the following is to be noted:
**see accompanying page**

**INTERNATIONAL PRELIMINARY REPORT**
**ACCOMPANYING PAGE**

## To SECTION V:

1). According to its title, the international application PCT/DE00/189 is concerned with a device and a method for secure electronic data processing. Claim 1 describes a device and the independent claim 12 the process.

2). The **nearest state of the art** according to the international search report are documents **D1** and **D2**.

**D1**: EP-A-0 869 652 (TUMBLEWEED SOFTWARE CORP) 7 October 1998 (1998-10-07)
**D2**: US-A-5 751 813 (DORENBOS DAVID) 12 MAY 1998 (1998-05-12)

The generic part of claim 1 is based on the disclosure of D2.

The drawback of the state of the art are explained on page 2, second and third paragraph as well as on page 6, lines 15 to 31.

- The **object of the invention** is (cf. Page 2, last paragraph) to provide a device and a method for secure data transmission via the server of a network wherein the addressee of the data does not need to be known at the time the data is available.

4a ). The object of the present invention is solved by the advantageous interaction of the technical features set forth in claim 1. The device of claim 1 is shown in figure 1.
Claim 1 states:
A device for secure transmission respectively forwarding of coded data
from a first data station
via a second data station
to a third data station of a network,
having
- an input unit
for receiving said coded data (10a) from said first data station
and
for receiving a requester's external key from said third or a further data station,
- a unit (2)
for recoding said coded data by means of decoding with an internal key and recoding with said external key, with said internal key not being accessible from outside said device:
and
- an output unit for issuing said data (10b) encoded with said external key,

**wherein**
said device is designed *in such a manner* on or in said second data station
that said unit (2) recodes the data only after request by said third data station with the aid of said requester's external key and
the data do not leave said device during recoding,
so that the data are not accessible in uncoded form on said second data station from outside said device.

4b). The objet of the present invention is solved by the advantageous interaction of the technical features set forth in independent claim 12.
Claim 12 states:
A method for secure transmission of data
from a first data station
via a second data station
to a third data station
using the *device according to one of the preceding claims* on
or in said second data station,
having the following steps:

- encoding the data **in said first data station** with a first key (10a),
- dividing said first key (10a) into a first part and a second part in such a manner that neither said first nor said second part alone permit decoding the coded data;
- encoding said first part of said first key (10a) in said first data station with the public key of said second data station;

- transmission of said coded data (11) together with said coded first part of said first key (10a) to said second data station;
- storage of said coded data (11) and of said coded first part of said first key (10a) **in said second data station;**
- request of said data by said third data station, the identity of which is unknown to said second data station until it is informed by the request;
- decoding of said coded first part of said first key in said second data station with a private key of said second data station matching said public key
  and
  recoding of said previously decoded first part of said first key with a public key of said third data station; and
- transmission of said coded data (11) together with said recoded first part of said first key (10b) to said third data station;

- decoding of said coded first part of said first key (10b) **in said third station** with a private key matching the public key of said third station;
- completion of said first key (10a) in said third station by adding said first part to said second part of said first key which was transmitted on a separate path from said first data station to said third data station;
- decoding said coded data (11) with the complete first key (10a) in said third data station.

5. The subject matter described in claims 1 and 12 develop advantageous effects as explained on page 7 (last paragraph) of the specification.

6. **None** of the documents of the international search report alone discloses all the technical features of claim 1 respectively of independent claim 12. The subject matter of claims 1 respectively 12 , therefore, fulfill the criterium of novelty (Art.33(10 and (2)PCT). The subject matter of claim 1 respectively 12 are also **not** obvious from the documents cited in the international search report. Therefore the requirements regarding inventive step of the claims subject matter are fulfilled (Article 33(1) and (3)PCT).
Commercial applicable is the subject matter of claims 1 respectively 13, i.a. in the field of

transmitting medical data. Consequently, the requirements of Article 33(1) and (4) PCT are fulfilled.

7. The dependent claims 2 to 11 and 13 to 16 define special designs of the device according to claim 1 respectively of the process according to claim 12, which principally and subject to the remarks in section VIII also fulfill the requirements with regard to novelty, inventive step and commercial applicability (Art. 33(2) to (4)PCT).

**To Section VII:**

1). Documents **D1** and **D2** were not cited in the specification; nor was the **state of the art** contained therein briefly described. The requirements of Rule 5.1(a)(ii)PCT are therefore not fulfilled.

2). The specification (cf. page 3, second paragraph ff.) was not adapted to the pertinent claims. Thus the requirements of Rule 5.1(a)(iii)PCT are not fulfilled.

3). Figure1/1 uses some expressions such as "receivers p'key" etc. which are not part of the language of the proceedings (German) and therefore do not fall in the category of known technical terms. These terms have to be replaced by understandable terms of the language of the proceedings. The English terms may continued to be used if set in brackets.

The applicant has said he will make respective amendments or adaptations upon entering in the regional or patenting phase.

**To Section VIII:**

The original, dependent claims 2 to 11 and 13 to 16 were not adapted to the amended independent claims 1 and 12. Thus there partly are objections regarding Article 6 PCT, because the additional features of the independent claims cause ambiguity (e.g. claim 13) or because the additional features of the independent claims have meanwhile become superfluous (e.g. claims 14 and 15) and the claims are therefore no longer concise.

The applicant has said he will make respective amendments or adaptations upon entering in the regional or patenting phase.

New Claims 1 and 12

1. A device for secure transmission respectively forwarding of coded data from a first data station via a second data station to a third data station of a network, having

- an input unit for receiving said coded data (10a) from said first data station and for receiving a requester's external key from said third or a further data station;
- a unit (2) for recoding said coded data by means of decoding with an internal key and renewed encoding with said external key, with said internal key not being accessible from outside said device; and
- an output unit for issuing said data (10b) encoded with said external key;

wherein said device is designed in such a manner on or in said second data station that said unit (2) recodes said data only upon request by said third data station with the aid of said requester's external key and said data do not leave said device during recoding, so that said data are not accessible in uncoded form on said second data station from outside said device.

12. A method for secure transmission of data from a first data station via a second data station to a third data station using the device according to one of the preceding claims on or in said second data station, having the following steps:

- encoding the data in said first data station with a first key (10a);
- dividing said first key (10a) into a first part and a second part in such a manner that neither said first nor said second part alone permit decoding the coded data;
- encoding said first part of said first key (10a) in said first data station with the public key of said second data station;
- transmission of said coded data (11) along with said coded first part of said first key (10a) to said second data station;

- storage of said coded data (11) and of said coded first part of said first key (10a) in said second data station;
- request of said data by said third data station, the identity of which is not conveyed to said second data station until requested;
- decoding of said coded first part of said first key in said second data station with a private key of said second data station matching said public key and recoding of said previously decoded first part of said first key with a public key of said third data station; and
- transmission of said coded data (11) along with said recoded first part of said first key (10b) to said third data station;
- decoding of said coded first part of said first key (10b) in said third station with a private key matching the public key of the third station;
- completion of said first key (10a) in said third data station by adding said first part to said second part of said first key which was transmitted on a separate path from said first data station to said third data station;
- decoding said coded data (11) with said complete first key (10a) in said third data station.

**PCT** WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04L 9/30, 9/08, 29/06

A1

(11) Internationale Veröffentlichungsnummer: **WO 00/59155**

(43) Internationales Veröffentlichungsdatum: 5. Oktober 2000 (05.10.00)

(21) Internationales Aktenzeichen: PCT/DE00/00189

(22) Internationales Anmeldedatum: 20. Januar 2000 (20.01.00)

(30) Prioritätsdaten:
199 14 225.4 29. März 1999 (29.03.99) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. [DE/DE]; Leonrodstrasse 54, D–80636 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: BRESSER, Bertram [DE/DE]; Augrät 32, D–66763 Dillingen (DE). PAUL, Volker [DE/DE]; A.–Weisgerber–Allee 144, D–66386 St. Ingbert (DE).

(74) Anwalt: GAGEL, Roland; Landsbergerstrasse 480a, D–81241 München (DE).

(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

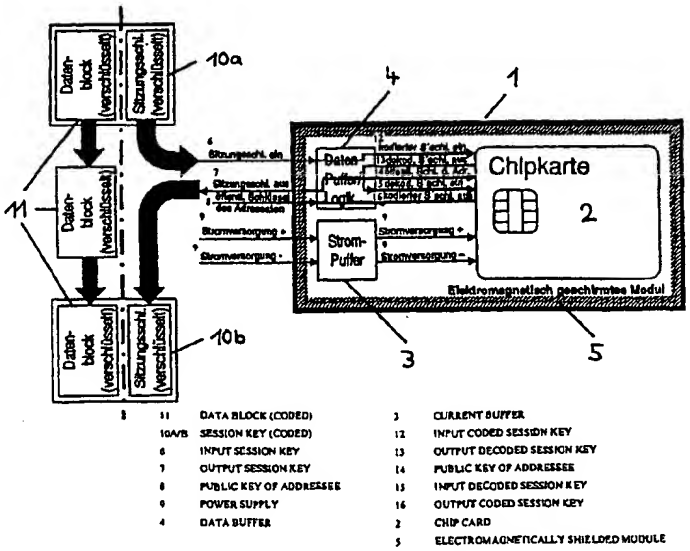
Veröffentlicht
*Mit internationalem Recherchenbericht.*

(54) Title: DEVICE AND METHOD FOR SECURE ELECTRONIC DATA TRANSMISSION

(54) Bezeichnung: VORRICHTUNG UND VERFAHREN FÜR DIE SICHERE ELEKTRONISCHE DATENÜBERTRAGUNG

(57) Abstract

The invention relates to a device and a method for the secure electronic transmission of data via the server of a network. According to said method the addressee of the data does not have to be known at the time the data are made available. The device, which has to be installed in the network server, comprises an input unit for receiving coded data (10a) and an external key. The device also comprises a unit (2) for decoding the coded data by means of an internal key and for the renewed encoding of the data using the external key. The internal key is not accessible from outside the device. The data (10b) encoded by means of the external key can be retrieved at the level of an output unit. The data can thus be read by the holder of the external key which in the course of a data request is transferred to the device together with the data, said holder also being the exclusive holder of the corresponding internal key.




(57) Zusammenfassung

Die vorliegende Erfindung betrifft eine Vorrichtung und ein Verfahren zur sicheren elektronischen Datenübertragung über den Server eines Netzwerkes, bei dem der Adressat der Daten zum Zeitpunkt der Bereitstellung der Daten noch nicht bekannt sein muß. Die Vorrichtung, die am Server des Netzwerkes installiert werden muß, weist eine Eingangseinheit zum Empfangen von verschlüsselten Daten (10a) sowie eines externen Schlüssels auf. Weiterhin ist in der Vorrichtung eine Einheit (2) zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel vorgesehen. Der interne Schlüssel ist von außerhalb der Vorrichtung nicht zugänglich. An einer Ausgangseinheit können die mit dem externen Schlüssel verschlüsselten Daten (10b) abgegriffen werden. Die Daten sind damit für den Inhaber des bei einer entsprechenden Datenanforderung mit den Daten an die Vorrichtung übergebenen externen Schlüssels und damit auch alleinigen Inhaber des zugehörigen internen Schlüssels lesbar.

*LEDIGLICH ZUR INFORMATION*

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albanien | ES | Spanien | LS | Lesotho | SI | Slowenien |
| AM | Armenien | FI | Finnland | LT | Litauen | SK | Slowakei |
| AT | Österreich | FR | Frankreich | LU | Luxemburg | SN | Senegal |
| AU | Australien | GA | Gabun | LV | Lettland | SZ | Swasiland |
| AZ | Aserbaidschan | GB | Vereinigtes Königreich | MC | Monaco | TD | Tschad |
| BA | Bosnien-Herzegowina | GE | Georgien | MD | Republik Moldau | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagaskar | TJ | Tadschikistan |
| BE | Belgien | GN | Guinea | MK | Die ehemalige jugoslawische Republik Mazedonien | TM | Turkmenistan |
| BF | Burkina Faso | GR | Griechenland | | | TR | Türkei |
| BG | Bulgarien | HU | Ungarn | ML | Mali | TT | Trinidad und Tobago |
| BJ | Benin | IE | Irland | MN | Mongolei | UA | Ukraine |
| BR | Brasilien | IL | Israel | MR | Mauretanien | UG | Uganda |
| BY | Belarus | IS | Island | MW | Malawi | US | Vereinigte Staaten von Amerika |
| CA | Kanada | IT | Italien | MX | Mexiko | | |
| CF | Zentralafrikanische Republik | JP | Japan | NE | Niger | UZ | Usbekistan |
| CG | Kongo | KE | Kenia | NL | Niederlande | VN | Vietnam |
| CH | Schweiz | KG | Kirgisistan | NO | Norwegen | YU | Jugoslawien |
| CI | Côte d'Ivoire | KP | Demokratische Volksrepublik Korea | NZ | Neuseeland | ZW | Zimbabwe |
| CM | Kamerun | | | PL | Polen | | |
| CN | China | KR | Republik Korea | PT | Portugal | | |
| CU | Kuba | KZ | Kasachstan | RO | Rumänien | | |
| CZ | Tschechische Republik | LC | St. Lucia | RU | Russische Föderation | | |
| DE | Deutschland | LI | Liechtenstein | SD | Sudan | | |
| DK | Dänemark | LK | Sri Lanka | SE | Schweden | | |
| EE | Estland | LR | Liberia | SG | Singapur | | |

# Vorrichtung und Verfahren für die sichere elektronische Datenübertragung

Die Erfindung betrifft eine Vorrichtung sowie ein Verfahren für die sichere elektronische Datenübertragung zwischen Endgeräten, die zeitweilig oder permanent mit einem Server verbunden sind.

Das Verfahren und die Vorrichtung sind insbesondere für die elektronische Weitergabe medizinischer Daten sehr gut geeignet.

Medizinische Daten stellen aus der rechtlichen Sicht des Datenschutzes eines der schützenswertesten Güter überhaupt dar. Für die elektronische Weitergabe medizinischer Daten über öffentlich zugängliche Netze, wie beispielsweise das Internet oder ein von außen zugängliches Verbundnetz, sind daher Sicherheitsmaßnahmen vorzusehen, die den bestmöglichen Schutz solcher Daten gewährleisten.

Die grundsätzlich für die Datenübertragung durch öffentliche Netze verfügbaren Sicherheitsmechanismen betreffen vor allem die Nutzung kryptographischer Verfahren zur Verschlüsselung der Daten. Hierbei werden in der Regel kryptographische Standardverfahren mit sicherem Austausch von Schlüsseln entsprechend X.509 eingesetzt. Dabei handelt es sich um symmetrische Verschlüsselungsverfahren, insbesondere für die Verschlüsselung großer Datenmengen, und um asymmetrische Verschlüsselungsverfahren unter Verwendung eines öffentlichen (sog. "public key") und eines

privaten Schlüssels (sog. "private key"), wie das weit verbreitete RSA.

Die vorliegende Erfindung betrifft die Übertragung von Daten von einem Netzteilnehmer (Absender) zu einem anderen (Adressat bzw. Empfänger) über die Zwischenspeicherung auf einer Datenstation bzw. einem Server. Während bei der elektronischen Datenübertragung über das Netz von einem Teilnehmer zu einem bereits bekannten Adressaten ein asymmetrisches Verschlüsselungsverfahren unter Verwendung des öffentlichen Schlüssels des Adressaten zur Verschlüsselung der Daten eine hohe Datensicherheit bietet, kann diese Vorgehensweise bei einem zum Zeitpunkt der Bereitstellung der Daten noch unbekannten Adressaten nicht eingesetzt werden.

Ein solcher Fall ergibt sich beispielsweise im medizinischen Bereich, wie weiter unten im Ausführungsbeispiel näher erläutert wird, wenn ein Arzt einem Patienten eine Überweisung an einen Kollegen ausstellt und die für den Arztkollegen bestimmten medizinischen Daten des Patienten auf elektronischem Wege bereitstellen will. Die Identität des Kollegen, den der Patient schließlich aufsuchen wird, ist zu diesem Zeitpunkt in vielen Fällen noch nicht bekannt.

Die Aufgabe der vorliegenden Erfindung besteht nun darin, eine Vorrichtung und ein Verfahren für die sichere elektronische Datenübertragung über den Server eines Netzwerkes bereitzustellen, bei dem der Adressat der Daten zum Zeitpunkt der Bereitstellung der Daten noch nicht bekannt sein muß.

Die Aufgabe wird mit der Vorrichtung und dem Verfahren nach den Ansprüchen 1 und 12 gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen des Verfahrens und der Vorrichtung sind Gegenstand der Unteransprüche.

Die erfindungsgemäße Vorrichtung, die am Server des Netzwerkes installiert und betrieben werden muß, weist eine Eingangseinheit zum Empfangen von verschlüsselten Daten (des Absenders) sowie eines externen Schlüssels (des Empfängers) auf. Weiterhin ist in der Vorrichtung eine Einheit zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel vorgesehen. Der interne Schlüssel ist innerhalb der Vorrichtung in irgendeiner technischen Form abgelegt und von außerhalb der Vorrichtung nicht zugänglich. An einer Ausgangseinheit können die mit dem externen Schlüssel verschlüsselten Daten abgegriffen werden.

Es versteht sich von selbst, daß die von der Vorrichtung zu verarbeitenden Daten so verschlüsselt sein müssen, daß sie mit dem internen Schlüssel der Vorrichtung entschlüsselt werden können. In der Vorrichtung werden somit nur für die Vorrichtung lesbare verschlüsselte Daten mit einem externen Schlüssel zur Neuverschlüsselung umgewandelt in neu verschlüsselte Daten, die für den Inhaber des bei einer entsprechenden Datenanforderung mit den Daten an die Vorrichtung übergebenen externen Schlüssels lesbar sind.

Hierbei ist es grundsätzlich möglich, die zu übertragenden Ursprungsdaten, d.h. beispielsweise medizinische Daten, von der Vorrichtung entschlüsseln sowie neu verschlüsseln zu lassen. Bei dem bevorzugten Einsatz der Vorrichtung, wie weiter unten ausgeführt, werden allerdings nicht die Ursprungsdaten selbst, sondern nur deren in verschlüsselter Form übertragener Schlüssel mit der Vorrichtung neu verschlüsselt.

In einer bevorzugten Ausführungsform weist die Vorrichtung zum Entschlüsseln der verschlüsselten Daten sowie zur Neuverschlüsselung der Daten eine Chipkarte als Träger des internen Schlüssels auf. Bei dieser Chipkarte handelt es sich vorzugsweise um eine Chipkarte eines zertifizierten Trust-Centers.

In einer weiteren Ausprägung können Verschlüsselung und Entschlüsselung ganz oder teilweise direkt durch eine aktive Chipkarte ausgeführt werden.

Eine weitere Möglichkeit besteht darin, eine nach dem Informations- und Kommunikationsdienste-Gesetz sowie Signaturgesetz geeignete Schaltung, gegebenenfalls Software-gesteuert als Einheit zur Ver- und Entschlüsselung einzusetzen.

Kern der erfindungsgemäßen Lösung ist eine Umschlüsselung der Daten oder eines den Daten anhängenden Schlüssels, im folgenden als Session-Key bezeichnet, so daß die Daten für einen der berechtigten Kommunikationspartner, den Adressaten, lesbar werden. Dazu wird in der bevorzugten Ausführungsform des Verfahrens ein für die symmetrische Verschlüsselung der Daten verwendeter Session-Key mit dem im Server vorhandenen priva-

ten Schlüssel des Servers entschlüsselt und sofort wieder mit dem öffentlichen Schlüssel des die Daten anfordernden Empfängers bzw. Adressaten verschlüsselt. Dieser Schlüssel ist vorzugsweise - z.B. zusammen mit der Teilnehmer-ID und der ISDN-Nummer - in einem Verzeichnis der beteiligten und berechtigten Netzteilnehmer auf dem Server gespeichert und kann bei Bedarf über die Dienste eines Trust-Centers jederzeit aktualisiert werden.

Ein Entschlüsseln der Ursprungsdaten selbst ist bei diesem Verfahren nicht notwendig. Zum späteren Entschlüsseln der Daten muß nur der - jetzt für den Empfänger lesbare - Session-Key bekannt sein, der bei der Verschlüsselung beispielsweise per Zufall generiert wurde, wie im Ausführungsbeispiel näher erläutert wird.

Auf diese Weise wird vermieden, daß die Daten selbst zu irgendeinem Zeitpunkt auf dem Server in unverschlüsselter Form vorliegen. Im Detail bedeutet dies, daß auf die verschlüsselten Daten während des Umschlüsselungsprozesses überhaupt kein Zugriff erfolgt. Verarbeitet wird lediglich der für Ihre Verschlüsselung verwendete Session-Key, der in einem geschlossenen Prozeß aus einer nur für den Server bzw. die am Server installierte erfindungsgemäße Vorrichtung lesbaren in eine für den Anfordernden lesbare Form "umgeschlüsselt" wird.

Der Einsatz der Vorrichtung soll im nachfolgenden anhand eines Ausführungsbeispiels in Verbindung mit der Figur näher erläutert werden. Dieses Beispiel betrifft einen Anwendungsfall im medizinischen Bereich, der ein

bevorzugtes Anwendungsfeld der vorliegenden Erfindung darstellt.

Hierbei werden in Kombination mit der erfindungsgemäßen Vorrichtung sowie dem erfindungsgemäßen Verfahren weitere, für sich genommen bereits bekannte Sicherheitsmaßnahmen beschrieben und vorgenommen, die insgesamt eine hochsichere Datenweitergabe in dem genannten Anwendungsfall gewährleisten.

Es versteht sich von selbst, daß die nachfolgend angeführten Kombinationen der einzelnen Sicherheitsmaßnahmen unabhängig voneinander sind, so daß auch die Auslassung eines dieser Schritte, oder der Ersatz durch andere bekannte Sicherheitsmaßnahmen, möglich sind.

Das Beispiel betrifft die elektronische Weitergabe medizinischer Daten über öffentliche Netze. Die hierfür eingesetzten Sicherheitsmaßnahmen gewährleisten den bestmöglichen Schutz dieser sensiblen Daten. Ein typischer Vorgang in diesem Bereich beginnt in der Praxis des Arztes eines Patienten. Der Arzt überweist den Patienten an einen Facharzt, der diesem aufgrund des freien Arztwahlrechtes des Patienten zu diesem Zeitpunkt noch nicht bekannt ist. Üblicherweise wurden dem Patienten bisher hierzu in einem verschlossenen Umschlag die für den Facharzt wichtigen medizinischen Daten zusammen mit der Überweisung übergeben, der diese dem von ihm gewählten Facharzt dann weitergegeben hat.

Wollte der Arzt diese Daten dem Kollegen auf elektronischem Wege übermitteln, so mußte er bisher die Identität dieses Kollegen zum Zeitpunkt der Überweisung bereits kennen. Dies ist mit dem im folgenden geschilderten Verfahren unter Einsatz der erfindungsgemäßen Vorrichtung und des erfindungsgemäßen Verfahrens nicht

mehr erforderlich. Das zugrunde liegende System sieht zumindest eine zentrale Datenstation, einen Server, vor, zu dem von Datenstationen der am System beteiligten Stellen, im vorliegenden Fall den externen Rechnern der Ärzte, eine Verbindung hergestellt werden kann. Bezogen auf den oben dargestellten Fall bedeutet dies, daß der überweisende Arzt die für den (noch unbekannten) Kollegen vorgesehenen medizinischen Daten des Patienten auf dem Server ablegt, von dem sich der Kollege diese Daten dann zu einem späteren Zeitpunkt holen kann.

Die Beschreibung der Sicherheitsmechanismen geht dabei zunächst von allgemeinen Sicherheitsaspekten des Systemdesigns aus, beschreibt dann die allgemeine und spezielle Nutzung kryptographischer Verfahren und schließlich die Einbindung und technische Umsetzung der erfindungsgemäßen Vorrichtung.

Jede Form des aktiven Lesens von Daten erfordert ein - gegebenenfalls eingeschränktes - Zugriffsrecht auf die Datenstation, auf der die Daten gespeichert sind. Im vorliegenden Beispiel gestattet das System keinen lesenden Zugriff auf den Server, sondern nur das Absetzen einer Datenanforderung durch die beteiligten Stellen. Bei nachgewiesener Empfangsberechtigung werden die Daten dem Anforderer, im vorliegenden Beispiel also dem die Daten anfordernden Facharzt, über das Netz zugeschickt. Dadurch werden direkte Zugriffe einer externen Stelle auf Datenbestände des Servers weitestgehend unterbunden.

Das beispielhafte Konzept verwendet für die Kommunikation eine Kommunikationsart, die als "remote procedure call" (RPC) bekannt ist. Dabei wird vom externen Rechner eine Aufforderung an den Server gesendet, eine bestimmte Funktion auszuführen und das Ergebnis dieser Funktion als Resultat zurückzugeben. Der Vorteil dieser Kommunikation ist, daß auf dem Server eine problemspezifische Applikation läuft, die nur genau die Operationen ausführt, die in der Systemfunktion vorgesehen sind. Darüber hinausgehende Funktionen, wie z.B. ein direkter Dateizugriff, sind auf diese Weise absolut sicher ausgeschlossen.

Das Konzept sieht weiterhin vor, daß ein Netzteilnehmer zum Aufbau einer Verbindung zunächst immer eine Aufforderung zum Verbindungsaufbau an den Server schickt. Bei dieser Operation selbst erfolgt noch kein Verbindungsaufbau. Es ist vielmehr vorgesehen, diese Anforderung als sogenannte "D-Kanal-Nachricht" zu realisieren. Dabei handelt es sich um eine spezielle Funktion des ISDN-Netzes, bei der noch vor dem "Annehmen" eines Gespräches - damit auch gebührenfrei - nur die Kennung bzw. Nummer des Anrufers übermittelt wird. Anschließend prüft der Server die Übereinstimmung dieser Nummer mit einer am Server gespeicherten Teilnehmerliste, und nur wenn die übermittelte Nummer des Anrufers zu einem "berechtigten" Netzteilnehmer gehört, initiiert der Server einen Rückruf über eine in einer internen Datenbank gespeicherte Nummer.

Der besondere Sicherheitsaspekt dieser Lösung besteht darin, daß zwar die im D-Kanal übertragene Nummer des Anrufers unter bestimmten Umständen

fälschbar ("maskierbar") ist, die Verbindung durch den Server aber in jedem Fall mit dem tatsächlichen Inhaber dieser Nummer, also einen berechtigten Netzteilnehmer aufgebaut wird. Damit wird im ungünstigsten Falle ein Verbindungsaufbau zu einem Netzteilnehmer angestoßen, der diesen gar nicht angefordert hatte, jedoch zum Kreis der Berechtigten gehört. In einem derartigen Fall kann es zu keiner Datenübertragung kommen, da der Rechner des unaufgefordert zurückgerufenen Teilnehmers keine Datenanforderung bereithält, und damit auch nicht zum Verbindungsaufbau bereit ist.

Das vorliegend beschriebene beispielhafte Konzept basiert darauf, Dokumente im Sinne eines "Mailings" einmalig zu übertragen. Sobald ein Dokument vom Server durch einen berechtigten Adressaten abgefordert und diesem zugestellt wurde, wird es auf dem Server gelöscht (zunächst logisch, dann auch physisch). Dies ist speziell im vorliegenden Anwendungsfall möglich, da die Daten jeweils nur für einen Adressaten vorgesehen sind. Sollen die Daten mehreren Adressaten zugänglich sein, wird diese Maßnahme nicht vorgesehen.

Alle Dokumente werden weiterhin mit einem Verfallsdatum versehen, nach dessen Ablauf sie ebenfalls physisch gelöscht werden. Damit entsteht keine Akkumulation von Daten auf dem Server, womit auch die Zusammenführung von unterschiedlichen Dokumenten, die etwas über einen Patienten oder auch über einen Arzt aussagen könnten, unmöglich gemacht wird. Die Identifikation der Dokumente erfolgt über eine einmalig nur für diesen Kommunikationsvorgang vergebene Vorgangs-ID, die keinen Rückschluß auf den Patienten zuläßt. Diese ID muß dem anfordernden Arzt bekannt sein, und wird ihm

vorzugsweise mit dem zugehörigen Papierdokument durch den Patienten übermittelt.

Zusätzlich zu den oben beschriebenen Sicherheitsmaßnahmen werden alle Daten für die Übertragung und Speicherung verschlüsselt und signiert. Dazu werden kryptographische Standardverfahren mit sicherem Austausch von Schlüsseln, beispielsweise entsprechend X.509, eingesetzt. Dabei handelt es sich um symmetrische Verschlüsselungsverfahren wie Triple DES, "blowfish" oder IDEA für die Verschlüsselung großer Datenmengen und asymmetrische Verschlüsselungsverfahren wie RSA oder elliptische Verschlüsselungsverfahren für die digitale Signatur (Verschlüsselung eines Hash-Wertes) und die Verschlüsselung des symmetrischen Session-Keys.

Zur Sicherung der Authentizität und Integrität der übertragenen Daten wird jedes Dokument vor dem Versand mit dem privaten Schlüssel des Absenders, im vorliegenden Fall des überweisenden Arztes, signiert. Dazu wird ein Hash-Wert ermittelt und dieser mit dem privaten Schlüssel des Absenders asymmetrisch verschlüsselt. Die Signatur des Dokumentes bleibt auch nach dem Entschlüsseln (siehe nachfolgende Schritte) erhalten und steht somit für den forensisch relevanten Nachweis der Echtheit des Dokumentes zur Verfügung. Voraussetzung für den Nachweis der Echtheit ist allerdings, daß das Dokument beim Empfänger in der signierten Form gespeichert wird, gegebenenfalls zusätzlich zur lesbaren Version ohne Signatur. Ein getrenntes Speichern von Dokument und Signatur ist möglich, birgt jedoch die Gefahr, daß durch ungewollte Modifikation des Dokumen-

tes - z.B. beim Öffnen im Textverarbeitungssystem - die Signatur ungültig wird. Die Archivierung des Dokuments obliegt dem Empfänger.

Die Einzeldokumente werden mit einem zufällig generierten Schlüssel (Session-Key) der Länge N (N sollte aus Sicherheitsgründen größer oder gleich 128 sein) symmetrisch verschlüsselt. Der zum Verschlüsseln verwendete Session-Key wird mit dem öffentlichen Schlüssel des Servers, d.h. der am Server installierten erfindungsgemäßen Vorrichtung, verschlüsselt. Die Schlüssellänge sollte aus Sicherheitsgründen mindestens 1024 Bit betragen.

Da das Dokument inklusive Signatur verschlüsselt wird, kann der Server ohne Entschlüsselung der Daten die Echtheit des Dokumentes - auch im Sinne seiner fehlerfreien Übertragung und seiner Existenz an sich (elektronisches "Einschreiben") - nicht überprüfen. Um dies zu ermöglichen, wird das signierte und verschlüsselte Dokument nochmals zusätzlich signiert.

Das wie oben beschrieben vorbereitete Dokument wird als MIME-kompatibles File aufbereitet und in dieser Form mittels eines entsprechenden RPC an den Server übermittelt.

Auf dem Server wird das Dokument aus dem MIME-Format entpackt und die äußere Signatur kontrolliert und dabei entfernt. Damit wird die Unversehrtheit, d.h. die Vollständigkeit und Originalität, des Dokumentes überprüft und kann protokolliert werden. Nach erfolgter Ablage des (verschlüsselten) Dokumentes wird eine vom

Server mit dessen persönlichem Schlüssel signierte Empfangsbestätigung an den Absender zurückgegeben als zweifelsfreier Nachweis der erfolgten Ablage des Dokumentes.

Das weiterzuleitende Dokument wird auf dem Server in der (innen) signierten und dann verschlüsselten Form gespeichert. In dieser verschlüsselten Form ist es von niemandem zu entschlüsseln.

Als Ablage- bzw. Zugriffskriterium zum Verwalten des verschlüsselten Dokuments dient eine unverschlüsselt mitgelieferte Vorgangs-ID, die zu jedem Vorgang gehört. Diese Vorgangs-ID, wird, wie bereits oben dargelegt, dem später durch den Patienten ausgewählten Arzt durch diesen auf direktem Wege übermittelt. Für den Server ist diese ID aus der übersandten Datenanforderung ersichtlich, deren Bestandteil sie ist.

Daten können vom Server durch Mitglieder des jeweiligen Netzes unter Angabe dieser jeweiligen Vorgangs-ID, ihrer ISDN-Nummer und ihrer Arztkennung angefordert werden.

Zur weiteren Erhöhung der Sicherheit können zusätzliche Identifikatoren, z.B zur Kennzeichnung des jeweiligen Patienten, notwendig sein.

Bei der Anforderung der Daten durch den betreffenden Facharzt erfolgt eine Umschlüsselung der Daten durch die erfindungsgemäße Vorrichtung, so daß sie für einen den anfordernden Arzt lesbar werden. Dazu wird der für die symmetrische Verschlüsselung der Daten verwendete Session-Key mit dem im Server vorhandenen privaten Schlüssel des Servers entschlüsselt und sofort

wieder mit dem öffentlichen Schlüssel des anfordernden Empfängers verschlüsselt. Dieser öffentliche Schlüssel ist - zusammen mit der Arzt-ID und der ISDN-Nummer - im Verzeichnis der beteiligten Netzärzte gespeichert und kann über die Dienste eines einbezogenen Trust-Centers jederzeit aktualisiert werden.

Ein Entschlüsseln der medizinischen Daten selbst ist nicht notwendig. Zum späteren Entschlüsseln der Daten muß nur der - jetzt für den Empfänger lesbare - Session-Key bekannt sein, der bei der Verschlüsselung per Zufall generiert wurde.

Auf diese Weise wird vermieden, daß die medizinischen Daten selbst zu irgendeinem Zeitpunkt auf dem Server in unverschlüsselter Form vorliegen. Auf die verschlüsselten Daten erfolgt während des Umschlüsselungsprozesses keinerlei Zugriff. Verarbeitet wird lediglich der für Ihre Verschlüsselung verwendete Session-Key, der in einem geschlossenen Prozeß aus einer nur für den Server lesbaren in eine für den Anfordernden lesbare Form "umgeschlüsselt" wird.

Das für den Versand an den Empfänger verschlüsselte Dokument wird nochmals zur Sicherung der korrekten Übertragung zum Empfänger und einer eventuell gewünschten Protokollierung signiert, und zwar durch den Server mit dessen persönlichem Schlüssel.

Das wie oben beschrieben vorbereitete Dokument wird wiederum als MIME-kompatibles File aufbereitet und in dieser Form als Rückgabewert eines RPC zur Datenanforderung an den Anforderer geschickt.

Beim Empfänger wird das Dokument aus dem MIME-Format entpackt und die äußere Signatur kontrolliert und dabei entfernt. Damit wird wiederum die Unversehrtheit, d.h. Vollständigkeit und Originalität, des Dokumentes überprüft. Eine vom Empfänger mit dessen persönlichem Schlüssel signierte Empfangsbestätigung wird an den Server zurückgegeben als zweifelsfreier Nachweis der erfolgten Übermittlung des Dokumentes.

Mittels des persönlichen Schlüssels des Empfängers kann dieser den verschlüsselten Session-Key entschlüsseln und mit diesem wiederum die Daten selbst. Danach liegen diese lesbar nur noch in der durch den Absender signierten Form vor.

Die Signatur des Ausgangsdokumentes dient der Nachweisbarkeit seiner Originalität. Um diese zu erhalten ist es notwendig, das Dokument in der signierten Form aufzubewahren.

Ein möglicher Angriffspunkt auf die Daten ist der private Schlüssel des Servers. Da alle eingelagerten Daten - genauer gesagt alle Session-Keys der eingelagerten Daten - mit demselben Schlüssel des Servers lesbar sind, lohnt sich ein Angriff auf diesen Schlüssel einerseits besonders, andererseits wird er durch die Menge vorliegender Daten erleichtert.

Um diesem Umstand vorzubeugen, wird bei einer bevorzugten Ausführungsform der vorliegenden Erfindung als zusätzlicher Sicherheitsmechanismus eine Zweiteilung des Session-Keys eingeführt.

Wie weiter oben beschrieben, werden die Ursprungsdaten mit einem N-stelligen (N vorzugsweise größer oder gleich 128) symmetrischen Schlüssel verschlüsselt. Dieser Schlüssel wird üblicherweise für die Übertragung asymmetrisch und nur für den Empfänger lesbar verschlüsselt. Die - auch gewaltsame - Entschlüsselung des Session-Keys reicht damit aus, um die Daten selbst entschlüsseln zu können.

Um dies zu verhindern, wird folgende Modifikation eingeführt. Bei dieser Modifikation wird der Session-Key vor seiner asymmetrischen Verschlüsselung zweigeteilt. Beispielsweise werden M ($0 < M < N$) der N Bits des Session-Keys als sogenannter "Vorgangsschlüssel" herausgelöst. Nur die verbleibenden (N-M) Bits des Session-Keys werden asymmetrisch verschlüsselt und mit den Daten übertragen.

Die Umschlüsselung der Daten mit reduziertem Session-Key kann in genau derselben Weise erfolgen, wie oben in Zusammenhang mit einem vollständigen Session-Key beschrieben. Da die Daten selbst auch dort nie entschlüsselt werden müssen, ist der vollständige Session-Key nicht notwendig. Es wird lediglich der rudimentäre Session-Key durch den Server entschlüsselt und für den Anforderer wieder verschlüsselt.

Die Entschlüsselung beim Empfänger unterscheidet sich von der oben beschriebenen Vorgehensweise dahingehend, daß nach der Entschlüsselung des Session-Keys mittels privatem Schlüssel des Empfängers dieser Session-Key um die beim Absender separierten M Bits des Vorgangsschlüssels erweitert werden muß. Danach kann die Entschlüsselung wie oben dargestellt erfolgen.

Der beim Absender der Daten erzeugte Vorgangsschlüssel, d.h. die separierten M Bits, wird an die ebenfalls dort erzeugte Vorgangs-ID angefügt. Die Kombination von Vorgangs-ID und Vorgangsschlüssel ergibt die sogenannte Vorgangskennung, die auf dem den Vorgang begleitenden Papierdokument (Überweisungschein, Einweisungsschein, Rezept, ...) aufgedruckt und beim Empfänger erfaßt wird. Der in der Vorgangskennung enthaltene Vorgangsschlüssel wird niemals zum Server übertragen, so daß dort nie alle Informationen zusammenkommen, die ausreichen würden, um ein Dokument tatsächlich zu entschlüsseln.

Ein Beispiel für eine erfindungsgemäße Vorrichtung, wie sie für die Durchführung des obigen Anwendungsbeispiels eingesetzt wird, ist in Figur 1 dargestellt.

Die Vorrichtung ist vorzugsweise in Form eines Einsteckmoduls 1 (Umschlüsselungsmodul) zum modularen Einbau in den Server ausgebildet. Das Modul 1 beinhaltet im vorliegenden Beispiel eine Chipkarte 2, die die Entschlüsselung des verschlüsselten Session-Keys 10a mit Hilfe des in der Chipkarte 2 gespeicherten privaten Schlüssels des Servers und die erneute Verschlüsselung des Session-Keys mit dem öffentlichen Schlüssel des Adressaten bzw. Anfordernden der Daten vornimmt. Der private Schlüssel des Servers ist dabei von außerhalb der Chipkarte bzw. des Moduls nicht zugänglich. Der öffentliche Schlüssel des Anfordernden wird der Vorrichtung 1, ebenso wie der umzuschlüsselnde Session-Key 10a über eine dafür vorgesehene Schnitt-

stelle zugeführt. Über eine weitere Schnittstelle wird der neu verschlüsselte Session-Key 10b ausgegeben.

Der Prozessor des Servers selbst übernimmt hierbei die Aufgabe, den Session-Key 10a von dem verschlüsselten Datenblock 11 abzutrennen, der Vorrichtung 1 zuzuführen und den von der Vorrichtung gelieferten, neu verschlüsselten bzw. umgeschlüsselten Session-Key 10b wieder an den Datenblock 11 anzufügen, wie in der Figur schematisch dargestellt ist.

Es ist allerdings auch möglich, diese Trennung und erneute Zusammenführung direkt in der Vorrichtung 1 vorzunehmen. Hierbei müßte der Vorrichtung der gesamte Datenblock 11 mit dem Session-Key 10a zugeführt werden.

Der persönliche Schlüssel des Servers ist zweifelsohne ein problematischer Punkt im Hinblick auf gezielte unberechtigte Zugriffsversuche auf die Daten.

Üblicherweise dürfen bzw. sollten Schlüssel nicht auf dem Rechner gespeichert werden, auf dem die verschlüsselten Daten gespeichert bzw. bearbeitet werden. Dies ist jedoch bei automatischer Arbeit des Servers, wie im vorliegenden Fall, unumgänglich. Aus diesem Grunde ist im vorliegenden Ausführungsbeispiel vorgesehen, die Vorrichtung als gekapselte und plombierte Einheit auszugestalten, die in der Lage ist, die vollständige Prozedur der Datenumschlüsselung intern zu handhaben, ohne daß der entschlüsselte (auch rudimentäre) Session-Key oder auch nur Spuren seiner Entschlüsselung die autonome Einheit verlassen.

Heutzutage sind bereits Schlüsselkarten am Markt verfügbar, die in der Lage sind, die asymmetrische Verschlüsselung eines 128 Bit Session-Keys nach einem

1024 Bit RSA-Verfahren vollständig auf dem Chip der Karte auszuführen. Demnächst werden solche Karten auch für 2048 Bit Schlüssel zur Verfügung stehen. Insbesondere besteht die Möglichkeit, das Schlüsselpaar (öffentlicher Schlüssel - privater Schlüssel) direkt auf der Karte oder in einem gesetzeskonformen, zertifizierten Trust-Center generieren zu lassen, ohne daß der private Schlüssel der Karte diese jemals verläßt. Eine solche Schlüsselkarte kann in der erfindungsgemäßen Vorrichtung als Chipkarte 2 eingesetzt werden. Hierbei wird dieser Karte 2 in einem ersten Schritt zunächst der verschlüsselte Session-Key 10a zugeführt. Dieser wird mit Hilfe des privaten Schlüssels des Karte, weiter oben als der private Schlüssel des Servers bezeichnet, entschlüsselt. Der entschlüsselte Session-Key wird von der Karte 2 ausgegeben, ohne die Vorrichtung 1 jedoch zu verlassen. Er wird vielmehr in einem zweiten Schritt der Karte 2 erneut, diesmal zusammen mit dem öffentlichen Schlüssel des Adressaten eingegeben. Die Karte 2 liefert in diesem zweiten Schritt den neu verschlüsselten Session-Key 10b zurück. Dies ist schematisch durch die Pfeile innerhalb der Vorrichtung 1 in der Figur angedeutet. Die hierfür zusätzlich erforderliche Schaltung, Puffer-Einheit 4, dient u.a. zur zeitlichen Koordination dieser Vorgänge. Diese Puffer-Einheit 4 kann beispielsweise durch einen geeignet programmierten Mikroprozessor oder mittels einer Logikschaltung realisiert werden.

Um zu verhindern, daß aus Modulationen auf der Stromversorgung der Vorrichtung Rückschlüsse auf die internen Abläufe möglich sind, ist in der vorliegenden Ausführungsform der Vorrichtung eine Konstant-

stromschaltung 3 vorgesehen, die garantiert, daß die Vorrichtung im Rahmen eines definierten Intervalls der Versorgungsspannung eine konstante und modulationsfreie Stromaufnahme vorweist. Bei Unter- oder Überschreiten bestimmter Grenzen der Betriebsspannung oder anderer Betriebsparameter, wie z.B. der Temperatur, schaltet sich die Vorrichtung mit einer Fehlermitteilung ab.

Da auch aus dem Zeitverhalten der Vorrichtung Rückschlüsse auf die internen Vorgänge gezogen werden könnten, können alle Eingangsdaten zunächst in der Puffer-Einheit 4 oder einer speziell dafür vorgesehenen Einheit gepuffert, und nach einer ständig gleichen Zeit die Ergebnisse ausgegeben werden, unabhängig davon, weiche Zeit die internen Abläufe in Anspruch genommen haben.

Ein "Abhören" der elektromagnetischen Vorgänge in der Vorrichtung wird im vorliegenden Ausführungsbeispiel durch eine elektromagnetische Abschirmung 5 der Vorrichtung verhindert.

Als Schnittstelle der Vorrichtung ist einerseits eine Schnittstelle für die Eingabe des asymmetrisch verschlüsselten Session-Keys 10a (bzw. des Rudimentes dieses Schlüssels) und des öffentlichen Schlüssels des anfordernden Empfängers vorgesehen. Andererseits muß eine Schnittstelle für die Ausgabe des asymmetrisch verschlüsselten Session-Keys 10b (bzw. dessen Rudiment) vorhanden sein. Beide Schnittstellen können bei geeigneter Ausführung physikalisch identisch sein.

Weiterhin können für die Erzeugung bzw. Überprüfung von Signaturen Schnittstellen für die

Eingabe des Hash-Wertes des zu signierenden Dokumentes und für die Ausgabe des symmetrisch verschlüsselten Hash-Wertes, d.h. der Signatur vorgesehen sein.

Obwohl die vorangehend beschriebenen Maßnahmen in Zusammenhang mit dem zugrunde liegenden Beispielfall dargestellt wurden, lassen sich dieses Konzept und die erfindungsgemäße Vorrichtung selbstverständlich auch auf andere Bereiche anwenden, bei denen eine sichere Datenübertragung zwischen zwei Datenstationen über eine Zwischenlagerung auf einem Server erforderlich ist.

Weiterhin ist die Erfindung nicht auf die Weiterleitung der Daten nur über eine Zwischenstation bzw. einen Server beschränkt. So können die Daten auch über mehrere Server geleitet werden, wobei der Abruf der Daten durch einen weiteren Server jeweils wie der Abruf durch einen Adressaten ausgeführt wird. Auf dem weiteren Server werden dann die Daten in gleicher Form wie auf dem ersten Server behandelt, d.h. auch dieser weitere Server muß die erfindungsgemäße Vorrichtung aufweisen.

Patentansprüche

1. Vorrichtung für die sichere Übertragung bzw. Weiterleitung von verschlüsselten Daten über eine Datenstation eines Netzwerkes, mit
- einer Eingangseinheit zum Empfangen der verschlüsselten Daten (10a) sowie eines externen Schlüssels,
- einer Einheit (2) zum Entschlüsseln der verschlüsselten Daten mit einem internen Schlüssel und zum erneuten Verschlüsseln der Daten mit dem externen Schlüssel, wobei der interne Schlüssel von außerhalb der Vorrichtung nicht zugänglich ist; und
- einer Ausgangseinheit zum Ausgeben der mit dem externen Schlüssel verschlüsselten Daten (10b).

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß der interne Schlüssel innerhalb der Einheit (2) zum Entschlüsseln und Verschlüsseln auf einem geeigneten Datenträger gespeichert ist.

3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln eine Chipkarte als Träger des internen Schlüssels umfaßt.

4. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln eine aktive Chipkarte mit integriertem Prozessor umfaßt, die die Ent- und Verschlüsselung der Daten ganz oder teilweise übernimmt.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß sie eine Puffer- und Logik-Einheit (4) zur zeitlichen Steuerung des Datenflusses in der Vorrichtung aufweist, die der Einheit (2) zum Entschlüsseln und Verschlüsseln zunächst die verschlüsselten Daten (10a) zur Entschlüsselung zuführt und entschlüsselt zurückerhält, und die anschließend der Einheit (2) zum Entschlüsseln und Verschlüsseln die entschlüsselten Daten zur Verschlüsselung mit dem externen Schlüssel zuführt und als verschlüsselte Daten (10b) zurückerhält.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Eingangseinheit und die Ausgangseinheit Standardschnittstellen für die Ein- und Ausgabe der Daten aufweisen.

7. Vorrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Einheit (2) zum Entschlüsseln und Verschlüsseln asymmetrische Verschlüsselungsverfahren einsetzt.

8. Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß sie mit einer vollständigen mechanischen und elektromagnetischen Kapselung (5) und mit einer Möglichkeit zur Versiegelung versehen ist.

9. Vorrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß eine Puffer-Einheit vorgesehen ist, die alle Datenströme innerhalb der Vorrichtung zum Ausgleich von eventuell vom internen Schlüssel abhängigen Verarbeitungszeiten puffert, so

daß die Ausgabe der Daten der Vorrichtung nach einer prozeßunabhängigen Zeitspanne erfolgt.

10. Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß eine Einheit (3) zum Puffern der Stromaufnahme der Vorrichtung vorgesehen ist, so daß die Stromaufnahme der Vorrichtung unabhängig von der vom internen Schlüssel abhängigen Stromaufnahme der Einheit (2) zum Entschlüsseln und Verschlüsseln oder weiterer interner Schaltkreise ist.

11. Vorrichtung nach einem der Ansprüche 1 bis 10, die weiterhin eine Einheit zum Empfangen eines ersten Datenblockes, der die verschlüsselten Daten (10a) neben weiteren Daten (11) beinhaltet, und zum Abtrennen der verschlüsselten Daten (10a) von den weiteren Daten (11) sowie eine Einheit zum Zusammenführen der weiteren Daten (11) mit den erneut verschlüsselten Daten (10b) zu einem zweiten Datenblock und zur Ausgabe des zweiten Datenblockes aufweist, wobei die verschlüsselten Daten einen Schlüssel darstellen, mit dem die weiteren Daten (11) verschlüsselt sind.

12. Verfahren für die sichere Übertragung von Daten von einer ersten Datenstation über eine zweite Datenstation zu einer dritten Datenstation unter Einsatz der Vorrichtung gemäß einem der vorangehenden Ansprüche, mit folgenden Schritten:

- Verschlüsseln der Daten in der ersten Datenstation mit einem ersten Schlüssel;
- Verschlüsseln zumindest eines Teils des ersten Schlüssels in der ersten Datenstation mit einem öffentlichen Schlüssel der zweiten Datenstation;

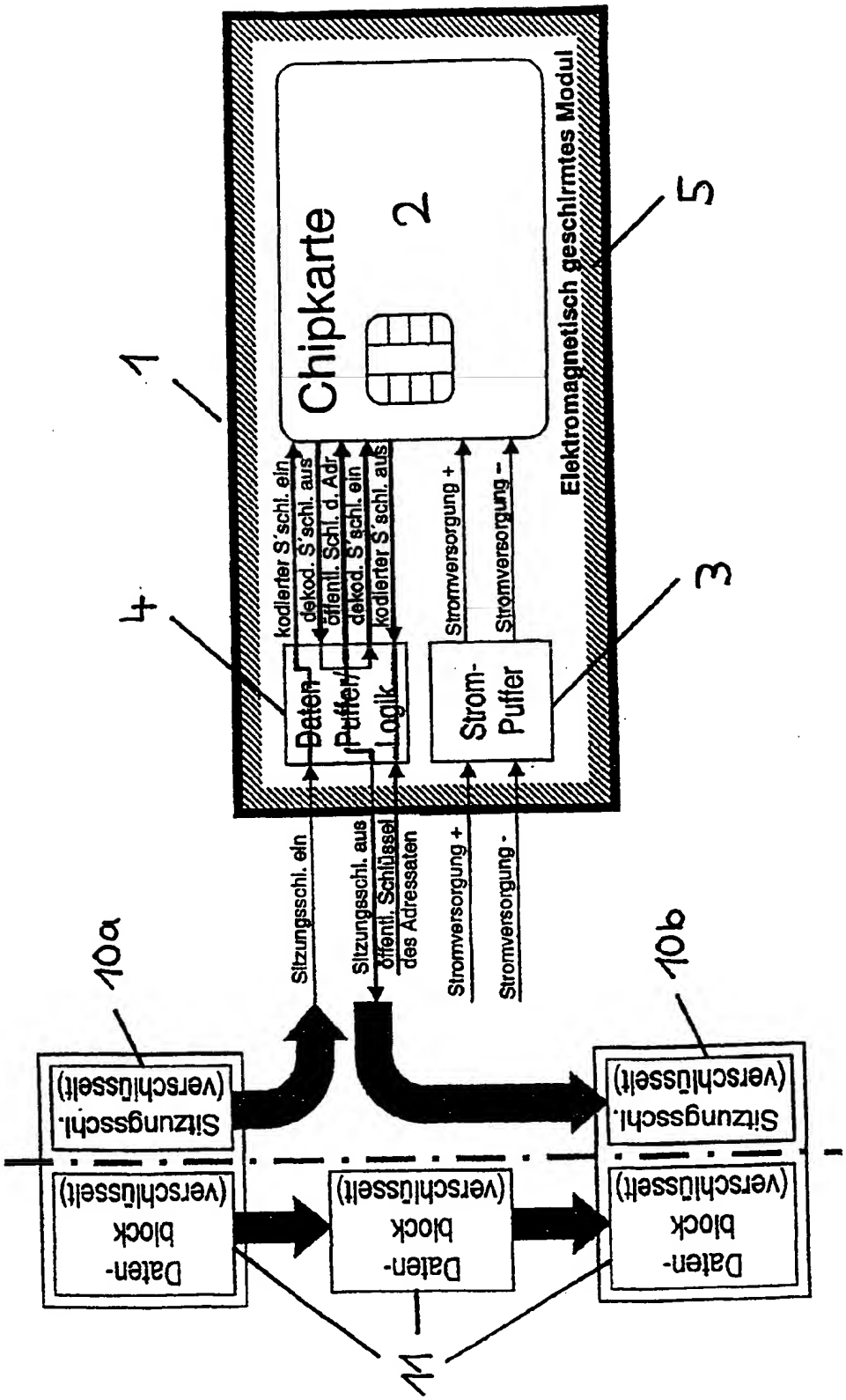
- Übermitteln der verschlüsselten Daten (11) zusammen mit dem verschlüsselten Teil des ersten Schlüssels (10a) an die zweite Datenstation;
- Speichern der verschlüsselten Daten (11) und des verschlüsselten Teils des ersten Schlüssels (10a) in der zweiten Datenstation;
- Anfordern der Daten durch die dritte Datenstation;
- Entschlüsseln des verschlüsselten Teils des ersten Schlüssels in der zweiten Datenstation mit einem zum öffentlichen Schlüssel passenden privaten Schlüssel der zweiten Datenstation und erneutes Verschlüsseln des vorher entschlüsselten Teils des ersten Schlüssels mit einem öffentlichen Schlüssel der dritten Datenstation; und
- Übermitteln der verschlüsselten Daten (11) zusammen mit dem erneut verschlüsselten Teil des ersten Schlüssels (10b) an die dritte Datenstation.

13. Verfahren nach Anspruch 12, wobei der erste Schlüssel vollständig verschlüsselt und übermittelt wird.

14. Verfahren nach Anspruch 12, wobei nur ein Teil des ersten Schlüssels verschlüsselt und an die zweite Datenstation übermittelt wird.

15. Verfahren nach einem der Ansprüche 12 bis 14, wobei der verschlüsselte Teil des ersten Schlüssels in der dritten Datenstation mit dem privaten Schlüssel der dritten Datenstation entschlüsselt wird, und anschließend die Daten (11) mit dem ersten Schlüssel entschlüsselt werden.

16. Verfahren nach einem der Ansprüche 12 bis 15, wobei der öffentliche Schlüssel der dritten Datenstation aus einer internen Datenbank der zweiten Datenstation entnommen oder durch Rückfrage bei einem Trust-Center ermittelt wird.




BERICHTIGTES BLATT (REGEL 91)

# INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/DE 00/00189

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30 H04L9/08 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 869 652 A (TUMBLEWEED SOFTWARE CORP) 7 October 1998 (1998-10-07)<br><br>page 14, line 42 -page 17, line 30; figure 3 | 1,2,6,7, 11-13, 15,16 |
| Y | --- | 3,4,8 |
| X | US 5 751 813 A (DORENBOS DAVID) 12 May 1998 (1998-05-12)<br>column 2, line 5 - line 67 | 1 |
| | --- | |
| | -/-- | |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 6 June 2000 | 28/06/2000 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Carnerero Álvaro, F |

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr ial Application No
PCT/DE 00/00189

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | ISHII S ET AL: "A HIGH-SPEED PUBLIC KEY ENCRYPTION PROCESSOR" SYSTEMS & COMPUTERS IN JAPAN,US,SCRIPTA TECHNICA JOURNALS. NEW YORK, vol. 29, no. 1, 1 January 1998 (1998-01-01), pages 20-31, XP000742968 ISSN: 0882-1666 page 20 page 26 | 3,4,8 |
| A | --- | 5,9,10 |
| A | MENEZES, VAN OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" , CRC PRESS , BOCA RATON, FLORIDA, USA; XP002139553ISBN: 0-8493-8523-7 page 524 -page 525 | 14 |
| | ---- | |

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

...formation on patent family members

Interr ...al Application No
PCT/DE 00/00189

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0869652 A | 07-10-1998 | US 6061448 A | 09-05-2000 |
| | | JP 11031127 A | 02-02-1999 |
| US 5751813 A | 12-05-1998 | AU 3877997 A | 19-11-1997 |
| | | BR 9702187 A | 29-06-1999 |
| | | CA 2224661 A | 06-11-1997 |
| | | EP 0882340 A | 09-12-1998 |
| | | JP 11509075 T | 03-08-1999 |
| | | PL 324266 A | 11-05-1998 |
| | | WO 9741661 A | 06-11-1997 |

# INTERNATIONALE[redacted]ECHERCHENBERICHT

Intern[redacted]ales Aktenzeichen
PCT/DE 00/00189

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**
IPK 7 H04L9/30 H04L9/08 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X | EP 0 869 652 A (TUMBLEWEED SOFTWARE CORP)<br>7. Oktober 1998 (1998-10-07)<br><br>Seite 14, Zeile 42 -Seite 17, Zeile 30;<br>Abbildung 3 | 1,2,6,7,<br>11-13,<br>15,16 |
| Y | --- | 3,4,8 |
| X | US 5 751 813 A (DORENBOS DAVID)<br>12. Mai 1998 (1998-05-12)<br>Spalte 2, Zeile 5 - Zeile 67 | 1 |
| | --- | |
| | -/-- | |

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 6. Juni 2000 | 28/06/2000 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Carnerero Álvaro, F |

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| Y | ISHII S ET AL: "A HIGH-SPEED PUBLIC KEY ENCRYPTION PROCESSOR" SYSTEMS & COMPUTERS IN JAPAN,US,SCRIPTA TECHNICA JOURNALS. NEW YORK, Bd. 29, Nr. 1, 1. Januar 1998 (1998-01-01), Seiten 20-31, XP000742968 ISSN: 0882-1666 Seite 20 Seite 26 | 3,4,8 |
| A | --- | 5,9,10 |
| A | MENEZES, VAN OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" , CRC PRESS , BOCA RATON, FLORIDA, USA; XP002139553ISBN: 0-8493-8523-7 Seite 524 -Seite 525 | 14 |
| | ----- | |

1

# INTERNATIONALER [redacted]CHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interna[redacted]les Aktenzeichen
PCT/DE 00/00189

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| EP 0869652 A | 07-10-1998 | US 6061448 A | 09-05-2000 |
| | | JP 11031127 A | 02-02-1999 |
| US 5751813 A | 12-05-1998 | AU 3877997 A | 19-11-1997 |
| | | BR 9702187 A | 29-06-1999 |
| | | CA 2224661 A | 06-11-1997 |
| | | EP 0882340 A | 09-12-1998 |
| | | JP 11509075 T | 03-08-1999 |
| | | PL 324266 A | 11-05-1998 |
| | | WO 9741661 A | 06-11-1997 |